LA-UR-97-834

Title:

SIMPLE, LOW-COST WAYS TO DRAMATICALLY IMPROVE THE SECURITY OF TAGS AND SEALS

Author(s):

R.G. JOHNSTON
A.R.E. GARCIA

Submitted to:

http://lib-www.lanl.gov/la-pubs/00418766.pdf

Los Alamos
NATIONAL LABORATORY

LAUR # 97-834

SIMPLE, LOW-COST WAYS TO DRAMATICALLY IMPROVE THE SECURITY OF TAGS AND SEALS

R.G. JOHNSTON and A.R.E. GARCIA
Los Alamos National Laboratory, Los Alamos, New Mexico U.S.A.

SIMPLE, LOW-COST WAYS TO DRAMATICALLY IMPROVE THE SECURITY OF TAGS AND SEALS

R.G. JOHNSTON and A.R.E. GARCIA
Los Alamos National Laboratory, Los Alamos, New Mexico U.S.A.

Tags and seals play an important role in international safeguards. Tags are materials or devices intended to uniquely mark or “fingerprint” an object (such as a container) so that it can reliably identified at a later date. This prevents the object from being confused with a similar looking object. Security seals, also called tamper-indicating devices, are meant to leave unambiguous, non-erasable evidence of unauthorized access.

The Vulnerability Assessment Team at Los Alamos National Laboratory has analyzed over 100 different tags and seals, ranging from simple and inexpensive products, through high-tech, complex devices. We have demonstrated how they can all be rapidly defeated (in 3 secs to 2 hours) using inexpensive, low-tech methods [1,2].

This work has led us to formulate some generic suggestions for optimizing the security and reliability of tags and seals. We believe that many of these suggestions can be implemented with minimal additional cost, and with only minor changes in the design of the products and/or how they are used. Some of these suggestions include:

- Users of tags and seals should have a clear understanding of their goals and what they want the tags/seals to accomplish. Periodically revisit these issues.

- There should be periodic vulnerability assessments [3], ideally conducted by outside, independent personnel psychologically predisposed to finding problems and suggesting useful counter-measures. These assessments should not be used to “certify” or “reject” certain products. Rather, vulnerability assessment should be thought of as a means for understanding the strengths and weaknesses of a tag/seal, for matching it to the most appropriate applications, and for optimizing reliability and security.

- Tags and seals should be viewed as only one part of an overall security or verification program. Discovering vulnerabilities in a tag or seal does not necessarily mean that the entire security/verification program has failed.

- Materials testing of a tag or seal--while useful--is not a substitute for a comprehensive vulnerability assessment [3].

- New tags and seals should undergo vulnerability assessments throughout the design process, not just when the product is complete and it is too late to make changes [3].

- Tag/seal inspectors should be familiar with the most likely attack scenarios associated with the tag/seal they are using, and specifically look or test for them.

- Tags or seals that are inspected visually should be examined with an identical tag or seal held right alongside. Humans do not accurately remember details of exact color, size, surface texture, and patterns, but they are very proficient at visual side-by-side comparisons.

- Tags and seals must be protected both before and after use. Discarded tags and seals, even if partially destroyed, provide potential adversaries with a useful source of information and counterfeit parts.

- If it is practical, used tags and seals should be archived for possible future analysis as new attacks are uncovered.

- Information about a tag or seal (such as the serial number) must not be stored in the container being protected, unless the information is encrypted.

- Manufacturers should not sell or provide free samples of seals lacking serial numbers. These are an excellent source for counterfeiting. Free samples should be a different color from the commercial product, or be blatantly marked in some other fashion.

- (Ideally the same) serial number should appear on every independent part of a seal. If serial numbers are stamped or embossed on a tag/seal, they should be done deeply enough that they can’t be easily buffed off.

- Simple physical attacks on high-tech systems are often highly effective because of the ease with which they can be accomplished, and because users/developers of high-tech systems often focus on other issues.

- The correlation coefficient, while commonly used, is often a poor algorithm for comparing “before” and “after” images for evidence of change [4]. On the other hand, blink comparators [5] can be simple and effective.

- Tags and seals based on adhesive labels should be protected for the first 48 hours after application, because of incomplete adhesion. (Heat can help speed up the process.) Users should clean the surface prior to application, and watch for surfaces that may have been pre-oiled or pre-coated to reduce adhesion. The adhesive, printing ink, and label substrate should be soluble in exactly the same solvents. The adhesive should melt at a higher temperature than the printing inks and substrate. Inspectors should examine not just the label, but the general area around the label. They should also pay particular attention to areas on the label that have not adhered to the surface, such as over slots, grooves, or screw holes.

ACKNOWLEDGMENTS

Kevin Grace, Ron Martinez, and George Eccleston offered useful suggestions.

REFERENCES

[1] JOHNSTON, RG, GARCIA, ARE, and GRACE, WK, Vulnerability Assessment of Passive Tamper-Indicating Seals, Journal of Nuclear Materials Management 224 (1995) 24-29.

[2] JOHNSTON, RG, and GARCIA, ARE, Vulnerability Assessment of Security Seals, Journal of Security Administration (in press).

[3] JOHNSTON, RG, Effective Vulnerability Assessment of Tamper-Indicating Seals, Journal of Testing and Evaluation (in press).

[4] YEN, EK and JOHNSTON, RG, The Ineffectiveness of the Correlation Coefficient for Image Comparisons (submitted).